对称加密算法

2020年3月14日 23:33

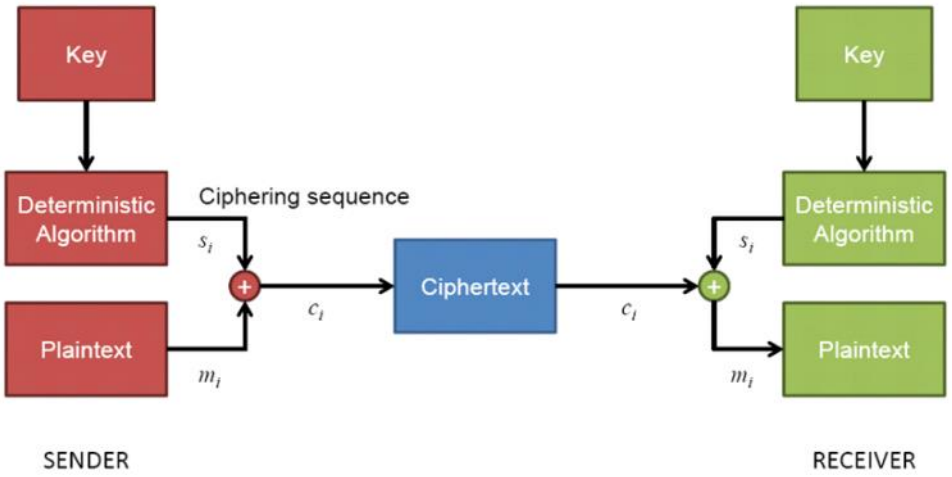
-
- 古典密码算法

1. 移位密码（Shift Cipher）：
   a. $e\_K\ (x)=(x+K)$ mod 26
   b. $d\_K\ (y)=(y-K)$ mod 26
   c. K取3时称为凯撒密码（Caesar）
2. 代换密码：
   a. 密钥空间大小为26!，让26个字母互相置换（映射）
   b. $e\_\pi\ (x)=\pi(x)$
   c. $d\_\pi\ (y)=\pi$^$(-1)\ (y)$
3. 仿射密码：
   a. 密钥空间$\mathcal{K}=\{(a,b)\in\mathbb{Z}_{26}\times\mathbb{Z}_{26}|\ \gcd(a,26)=1\}$
   b. $e\_K\ (x)=(ax+b)$ mod 26
   c. $d\_K\ (y)=a$^$(-1)\ (y-b)$ mod 26
4. 维吉尼亚密码(Vigenère密码)：
   a. 在$\mathbb{Z}$^26上进行不同下标不同移位量的移位加密：
   b. $e\_K\ (x\_1,x\_2,\cdots,x\_m\ )=(x\_1+k\_1,x\_2+k\_2,\cdots,x\_m+k\_m)$
   c. $d\_K\ (y\_1,y\_2,\cdots,y\_m\ )=(y\_1-k\_1,y\_2-k\_2,\cdots,y\_m-k\_m)$
5. 希尔密码：
   a. 密钥是mxm可逆矩阵，加密解密算法是乘以矩阵和乘以逆
6. 置换密码：
   a. 相当于洗牌打乱顺序
   b. $e\_K\ (x\_1,\cdots,x\_m\ )=(x\_\pi(1)\ ,\cdots,x\_(\pi(m)))$
   c. $d\_K\ (y\_1,\cdots,y\_m\ )=(y\_(\pi$^$(-1)\ (1)\ ),\cdots,y\_(\pi$^$(-1)\ (m)))$
7. 一次一密（one time pad）
   a. 每次都按位异或一个不同的密码

-
- 对称密码算法

1. 对称密码算法：消息的发送者和接收者使用相同的密钥进行加密和解密的算法。这个密钥通常被称为共享密钥或秘密密钥。
   a. 流密码stream cipher：对明文消息按比特位进行加密（有些情况是按字节进行加密），如RC4，ZUC，A5等
   b. 分组密码block cipher：对明文以分组为单位进行加密，每个明文分组通常是64比特或128比特，如DES，AES，Blowfish， Twofish，Skipjack，和RC2，又如轻量级分组密码：LBlock，Present，SIMON，SPECK，LED等

2. DES
    a. 典型的分组密码
    b. 明文分组长度64位
    c. 密钥长度64位，其中8比特作为校验位，因此有效长度为56比特
    d. 整体结构：解密过程 除了子密钥输出的顺序相反外，密钥调度的过程与加密完全相同
    e. 特点：灵活、多模式、不能提供足够的安全性能、运算量小、加密速度快、加密效率高
    f. 缺点：有很强的雪崩效应（明文或密钥的微小改变将对密文产生很大的影响）
    g. 弱点：
        i. 弱密钥：DES中存在着少量弱密钥，使得一个主密钥可以产生的所有子密钥都是一样的
        ii. 密文与明文、密文与密钥的相关性：每个密文位都是所有明文位和所有密钥位的复合函数，达到这一要求所需的迭代次数最少为5，迭代8次以后输出的输入就可认为是不相关的了
3. 多重DES
    a. 二重DES：用两个密钥各做一次加密，用中间相遇攻击只需2^57次即可破
    b. 三重DES：用三个或两个密码做加密解密加密
4. 穷尽密钥搜索攻击DES：
    a. DES的密钥个数：2^56≈〖10〗^17；
    b. 1997年1月28日，美国RSA数据安全公司悬赏10000美元破译密钥长度为56比特的DES；
    c. 从1997年3月13日起，美国科罗拉多州的程序员Verser用了96天成功破译了DES算法；
    d. 1998年7月，电子边境基金会(EFF)使用了25万美元的计算机在56小时内破解了56比特DES；
    e. 1999年1月，电子边境基金会(EFF)宣布花了22.5小时破解了DES；
5. 对称密码算法存在的问题
    a. 密钥管理成为用户的负担
    b. 对拥有庞大用户数量的网络的通信空间提出了很高的要求
    c. 密钥不能被及时更换以保证信息的保密性
    d. 数据的完整性得不到保证
    e. 无法保证接收到的消息来自于声明的发送者
6. AES评选过程
    a. 1997年1月2日，NIST开始遴选DES的替代者；
    b. 1998年8月20日，第一次AES候选大会上宣布了15个 AES的候选算法；
    c. 1999年5月，5个候选算法留下： MARS，RC6， Rijndael，Serpent，Twofish；
    d. 2000年10月2日，比利时研究者Daemen和Rijmen设计的Rijndael被选为高级数据加密标准；

7. AES评判的原则：安全性、代价、算法与实现特性，及NIST的评估结果
    a. 一般安全性：不存在已知的攻击；
    b. 软件执行：非常利于在包括8位和64位以及DSP在内的各种平台上执行的加密和解密算法；
    c. 适合在受限空间环境中执行加密或解密操作，对RAM和ROM的要求低；
    d. 硬件执行：在最后5个算法中，Rijndael在反馈模型下执行的速度最快，在非反馈模型下，执行速度位居第二；
    e. 对执行的攻击：非常利于防止能量攻击和计时攻击；
    f. 加密与解密：加解密执行速度差不多；
    g. 密钥灵活性：支持加密中的快速子密钥计算；
    h. 其他的多功能性和灵活性：支持128位，192位和256位组合。
    i. 指令级并行执行潜力。
8. 序列密码
    a. 原理关键：产生密钥流的算法，该算法必须能够产生可变长的、随机的、不可预测的密钥流。不是真随机序列
    b. 

    c. 与一次一密的区别：一次一密要求真正随机数流
    d. 密钥流周期要长
    e. 密钥流应尽可能地接近于一个真正的随机数流的特征
    f. 伪随机数发生器的输出取决于输入的密钥的值
9. RC4
    a. 是Ron Rivest为RSA公司在1987年设计的一种序列密码，它是一种可变密钥长度、面向字节操作的序列密码。
    b. 密码周期大于10^100；
    c. 被用于SSL/TLS标准，也用于IEEE802.1无线局域网中的WEP协议；
    d. RC4算法的优点是简单高效，特别适合软件实现。
    e. 初始化：

f.

```
for i from 0 to 255
    S[i] := i
endfor
j := 0
for i from 0 to 255
    j := (j + S[i] + key[i mod keylength]) mod 256
    swap values of S[i] and S[j]
endfor
```

g. 密钥生成：

h.

```
i := 0
j := 0
while GeneratingOutput:
    i := (i + 1) mod 256
    j := (j + S[i]) mod 256
    swap values of S[i] and S[j]
    K := S[(S[i] + S[j]) mod 256]
    output K
endwhile
```

10. 对称密码算法的问题
    a. 密钥管理成为用户的负担
    b. 对拥有庞大用户数量的网络的通信空间提出了很高的要求
    c. 密钥不能被及时更换以保证信息的保密性
    d. 数据的完整性得不到保证
    e. 无法保证接收到的消息来自于声明的发送者